

State succinctness of two-way finite automata with quantum and classical states

Shenggen Zheng^{1,*}, Daowen Qiu^{1,2,3,†}, Lvzhou Li^{1, ‡}

¹*Department of Computer Science, Sun Yat-sen University, Guangzhou 510006, China*

²*SQIG-Instituto de Telecomunicações, Departamento de Matemática, Instituto Superior Técnico, TULisbon, Av. Rovisco Pais 1049-001, Lisbon, Portugal*

³*The State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 100080, China*

Abstract

Two-way quantum automata with quantum and classical states (2QCFA) were introduced by Ambainis and Watrous in 2002. In this paper we study state succinctness of 2QCFA. For any fix $m \in \mathbb{Z}^+$, we show that

1. there is a promise problem A^{meq} which can be solved by 2QCFA in polynomial expected running time with one-sided error with constant numbers of quantum and classical states, whereas the sizes of the corresponding *deterministic finite automata* (DFA), *two-way nondeterministic finite automata* (2NFA) and polynomial expected running time *two-way probabilistic finite automata* (2PFA) are at least $2m + 2$, $\sqrt{\log m}$ and $\sqrt[3]{(\log m)/b}$;
2. there exists a language L^{mtwin} which can be recognized by 2QCFA in exponential expected running time with one-sided error with constant numbers of quantum and classical states, whereas the sizes of the corresponding DFA, 2NFA and polynomial expected running time 2PFA are at least 2^m , \sqrt{m} and $\sqrt[3]{m/b}$;

where b is a constant number.

Keywords: Computing models; Quantum finite automata; State complexity; Succinctness.

**E-mail address:* zhengshenggen@gmail.com

†Corresponding author. *E-mail address:* issqdw@mail.sysu.edu.cn (D. Qiu)

‡*E-mail address:* lilvzhou@gmail.com

1 Introduction

An important way to get a deeper insight into the power of various quantum resources and features for information processing is to explore power of various quantum variations of the basic models of classical automata. Of special interest and importance is to do that for various quantum variations of classical finite automata because quantum resources are not cheap and quantum operations are not easy to implement. Attempts to find out how much one can do with very little of quantum resources and consequently with the simplest quantum variations of classical finite automata are therefore of particular interest. This paper is an attempt to contribute to such line of research.

There are two basic approaches of how to introduce quantum features to classical models of finite automata. The first one is to consider quantum variants of the classical *one-way (deterministic) finite automata* (1FA or 1DFA) and the second one is to consider quantum variants of the classical *two-way finite automata* (2FA or 2DFA). Already the very first attempts to introduce such models, by Moore and Crutchfields [21] and Kondacs and Watrous [15] demonstrated that in spite of the fact that in the classical case, 1FA and 2FA have the same recognition power, this is not so for their quantum variations. Moreover, already the first important model of *two-way quantum finite automata* (2QFA), namely that introduced by Kondacs and Watrous, demonstrated that very natural quantum variants of 2FA are much too powerful - they can recognize even some *non-context free languages* and are actually not really finite in a strong sense [15]. It started to be therefore of interest to introduce and explore some “less quantum” variations of 2FA and their power [1, 2, 3, 9, 7, 18, 19, 20, 22, 24, 28, 29, 31, 32, 33].

A very natural “hybrid” quantum variations of 2FA, namely, *two-way quantum automata with quantum and classical states* (2QCFA) were introduced by Ambainis and Watrous [3]. Using this model they were able to show in an elegant way that an addition of a single qubit to a classical model can enormously increase power of automata. A 2QCFA is essentially a classical 2FA augmented with a quantum memory of constant size (for states in a fixed Hilbert space) that does not depend on the size of the (classical) input. In spite of such a restriction, 2QCFA have been shown to be more powerful than *two-way probabilistic finite automata* (2PFA) [3].

State complexity and succinctness results are an important research area of classical automata theory, see [34], with a variety of applications. Once quantum versions of classical automata were introduced and explored, it started to be of large interest to find out through succinctness results a relation between the power of classical and quantum automata model. This has turned out to be an area of surprising outcomes that again indicated that relations between classical and corresponding quantum automata models is intriguing. For example, it has been shown, see [2, 4, 5, 6, 17], that for some languages 1QFA require exponentially less states than classical 1FA, but for some other languages it can be in an opposite way.

Because of the simplicity, elegance and interesting properties of the 2QCFA model, as well as its natural character, it seems to be both useful and interesting to explore state complexity and succinctness results of 2QCFA and this we will do in this paper.

In the first part of this paper, 2QCFA are recalled formally and some basic notations are given. Then we will prove state succinctness result of 2QCFA on an infinite family of promise promises. For any fix $m \in \mathbb{Z}^+$ and any $\epsilon > 0$, let $A_{yes}^{meq} = \{w \in \{a, b\}^* | w = a^m b^m\}$ and $A_{no}^{meq} = \{w \in \{a, b\}^* | w \neq a^m b^m \text{ and } |w| \geq m\}$. We will prove that promise problem $A^{meq} = (A_{yes}^{meq}, A_{no}^{meq})$ can be solved by 2QCFA with one-sided error ϵ with constant numbers of quantum and classical states in polynomial expected running time, whereas the sizes of the corresponding DFA, 2DFA and 2NFA at least are $2m+2$, $\sqrt{\log m}$ and $\sqrt{\log m}$. We also show that for every $\epsilon < 1/2$ and any fix $m \in \mathbb{Z}^+$, any 2PFA solves promise problem A^{meq} with bounded error ϵ and within polynomial expected running time has least $\sqrt[3]{(\log m)/b}$ states, where $b > 0$ is a constant number. Finally, we show state succinctness result of 2QCFA on an infinite family of languages. For any fix $m \in \mathbb{Z}^+$ and any error bound $\epsilon > 0$, there exists a 2QCFA \mathcal{A} recognizes language $L^{mtwin} = \{wcw | w \in \{a, b\}^*, |w| = m, \Sigma = \{a, b, c\}\}$ with one-sided error ϵ with constant numbers of quantum and classical states in exponential expected running time. We use the lower bounds in the area of communication complexity to prove that any DFA recognizes language L^{mtwin} has at least 2^m . Next, we prove the sizes of corresponding 2DFA and 2NFA to recognize L^{mtwin} are at least \sqrt{m} . We also show that for every $\epsilon < 1/2$ and any fix $m \in \mathbb{Z}^+$, any 2PFA recognizes L^{mtwin} with bounded error ϵ and within polynomial expected running time has least $\sqrt[3]{m/b}$ states, where $b > 0$ is a constant number.

We now outline the remainder of this paper. Definitions of 2QCFA are recalled in Section 2. In Section 3 we prove state succinctness result of 2QCFA on an infinite family of promise promises. We show state succinctness result of 2QCFA on an infinite family of languages in Section 4. Finally, Section 5 is a conclusion, which includes mention of open problems relating to this paper.

2 Preliminaries

In the first part of this section we formally recall the model of 2QCFA. Concerning the basics of *quantum computation* we refer the reader to [13, 23] and concerning the basic properties of automata models we refer the reader to [13, 14, 25, 27].

2.1 Definition of 2QCFA

2QCFA were first introduced by Ambainis and Watrous [3], and then studied by Qiu, Yakaryilmaz and etc. [26, 31, 35, 36, 37]. Informally, we describe a 2QCFA as a 2DFA which has

access to a quantum memory of a constant size (dimension), upon which it performs quantum transformations and measurements. Given a finite set of quantum states Q , we denote by $\mathcal{H}(Q)$ the Hilbert space spanned by Q . Let $\mathcal{U}(\mathcal{H}(Q))$ and $\mathcal{O}(\mathcal{H}(Q))$ denote the sets of unitary operators and projective measurements over $\mathcal{H}(Q)$, respectively.

Definition 1. A 2QCFA \mathcal{A} is specified by a 9-tuple

$$\mathcal{A} = (Q, S, \Sigma, \Theta, \delta, q_0, s_0, S_{acc}, S_{rej}) \quad (1)$$

where:

1. Q is a finite set of quantum states;
2. S is a finite set of classical states;
3. Σ is a finite set of input symbols; Σ is then extended to the tape symbol set $\Gamma = \Sigma \cup \{\phi, \$\}$, where $\phi \notin \Sigma$ is called the left end-marker and $\$ \notin \Sigma$ is called the right end-marker;
4. $q_0 \in Q$ is the initial quantum state;
5. $s_0 \in S$ is the initial classical state;
6. $S_{acc} \subset S$ and $S_{rej} \subset S$ are the sets of classical accepting states and rejecting states, respectively.
7. Θ is the transition function of quantum states:

$$\Theta : S \setminus (S_{acc} \cup S_{rej}) \times \Gamma \rightarrow \mathcal{U}(\mathcal{H}(Q)) \cup \mathcal{O}(\mathcal{H}(Q)). \quad (2)$$

Thus, $\Theta(s, \gamma)$ corresponds to either a unitary transformation or a projective measurement.

8. δ is the transition function of classical states. If $\Theta(s, \gamma) \in \mathcal{U}(\mathcal{H}(Q))$, then δ is

$$S \setminus (S_{acc} \cup S_{rej}) \times \Gamma \rightarrow S \times \{-1, 0, 1\}, \quad (3)$$

which is similar to the transition function for 2DFA, where $\delta(s, \gamma) = (s', d)$ means that when the classical state $s \in S$ scanning $\gamma \in \Gamma$ is changed to state s' , and the movement of the tape head is decided by d . If $\Theta(s, \gamma) \in \mathcal{O}(\mathcal{H}(Q))$ which is a projective measurement, assume that the projective measurement with the set of possible eigenvalues $R = \{r_1, \dots, r_n\}$ and the projector set $\{P(r_i) : i = 1, \dots, n\}$ where $P(r_i)$ denotes the projector onto the eigenspace corresponding to r_i . Then δ is

$$S \setminus (S_{acc} \cup S_{rej}) \times \Gamma \times R \rightarrow S \times \{-1, 0, 1\}, \quad (4)$$

where $\delta(s, \gamma)(r_i) = (s', d)$ means that when the projective measurement result is r_i , the classical state $s \in S$ scanning $\gamma \in \Gamma$ is changed to state s' , and the movement of the tape head is decided by d .

Given an input w , a 2QCFA $\mathcal{A} = (Q, S, \Sigma, \Theta, \delta, q_0, s_0, S_{acc}, S_{rej})$ proceeds as follows:

At the beginning, the tape head is positioned on ϕ , the quantum initial state is $|q_0\rangle$, the classical initial state is s_0 , and $|q_0\rangle$ will be changed according to $\Theta(s_0, \phi)$.

- a. If $\Theta(s_0, \phi) = U \in \mathcal{U}(\mathcal{H}(Q))$, then the quantum state evolves as $|q_0\rangle \rightarrow U|q_0\rangle$, and meanwhile, the classical state s_0 is changed to s according to $\delta(s_0, \phi_1) = (s, d)$. The movement of the tape head is decided by d .
- b. If $\Theta(s_0, \phi_1) = M \in \mathcal{O}(\mathcal{H}(Q))$, then the measurement M is performed on $|q_0\rangle$. Let $M = \{P_1, \dots, P_m\}$ with result set $R = \{r_i\}_{i=1}^m$. After the measurement M has been performed, we get a result $r_i \in R$ with probability $p_i = \langle q_0 | P_i | q_0 \rangle$, and the quantum state $|q_0\rangle$ changes to $P_i|q_0\rangle/\sqrt{p_i}$. Meanwhile, the classical state changes according to $\delta(s_0, \phi)(r_i) = (s_i, d)$. If $s_i \in S_{acc}$ (S_{rej}), \mathcal{A} accepts (rejects) w and halts; otherwise, the tape head of \mathcal{A} moves according to the direction d , and continues to read the next symbol.

A computation is assumed to halt if and only if an accepting state or a rejecting classical state is entered.

Let $L \subset \Sigma^*$ and $0 \leq \epsilon < 1/2$. A 2QCFA \mathcal{A} recognizes L with one-sided error if

1. $\forall w \in L, \Pr[\mathcal{A} \text{ accepts } w] = 1$, and
2. $\forall w \notin L, \Pr[\mathcal{A} \text{ rejects } w] \geq 1 - \epsilon$.

2.2 Notations and some lemmas used in this paper

In this subsection we review some notations of 2QCFA [26]. For convenience, let $2QCFA_\epsilon$ denote the classes of all languages recognized by 2QCFA with given error probability ϵ and $2QCFA_\epsilon(ptime)$ denote the classes of all languages recognized by 2QCFA with given error probability ϵ which run in polynomial expected time. Moreover, let $QS(\mathcal{A})$ and $CS(\mathcal{A})$ denote the numbers of quantum states and classical states of a 2QCFA \mathcal{A} and let $T(\mathcal{A})$ denote the expected running time of 2QCFA \mathcal{A} . For a string w , the length of w is denoted by $|w|$.

Lemma 1 ([3]). *For any $\epsilon > 0$, there is a 2QCFA \mathcal{A} that accepts any $w \in L^{eq} = \{a^m b^m | m \in \mathbb{N}\}$ with certainty, rejects any $w \notin L^{eq}$ with probability at least $1 - \epsilon$ and halts in expected running time $\mathbf{O}(n^4)$ where $n = |w|$ is the length of the input w .*

Remark 1. According to the proof of Lemma 1 in [3], for the above 2QCFA we further have $QS(\mathcal{A}) = 2$, $CS(\mathcal{A}) = k$ where k is a constant.

Lemma 2 ([26]). *If $L_1 \in 2QCFA_{\epsilon_1}(ptime)$ and $L_2 \in 2QCFA_{\epsilon_2}(ptime)$, then $L_1 \cap L_2 \in 2QCFA_\epsilon(ptime)$, where $\epsilon = \epsilon_1 + \epsilon_2 - \epsilon_1\epsilon_2$.*

Lemma 3 ([14]). *Every n -state 2DFA can be simulated by a DFA with $(n+1)^{n+1}$ states.*

Lemma 4 ([8]). *Every n -state 2NFA can be simulated by a DFA with $2^{(n-1)^2+n}$ states.*

Lemma 5 ([10]). *For every $\epsilon < 1/2$, $a > 0$ and $d > 0$, there exists a constant $b > 0$ such that, for any c , if L is recognized by a c -state 2PFA with error probability ϵ and within time an^d then L is recognized by some DFA with at most c^{bc^2} states, where $n = |w|$ is the length of the input.*

Lemma 6 ([11]). *Let $A, B \subseteq \Sigma^*$ with $A \cap B = \emptyset$. Suppose there is an infinite set I of positive integers and, for each $m \in I$, a set $W_m \subseteq \Sigma^*$ such that*

- (1) $|w| \leq m$ for all $w \in W_m$,
- (2) for every integer k , there is an m_k such that $|W_m| \geq m^k$ for all $m \in I$ with $m \geq m_k$, and
- (3) for every $m \in I$ and every $w, w' \in W_m$ with $w \neq w'$, there are words $u, v \in \Sigma^*$ such that either $uwv \in A$ and $uw'v \in B$ or $uwv \in B$ and $uw'v \in A$.

Then no 2PFA separates A and B .

We recall some basic notations of *communication complexity*, we refer the reader to [16] for more details. Let X, Y, Z be arbitrary finite sets, consider a two-argument function $f : X \times Y \rightarrow Z$. Let Alice and Bob be the two communicating parties. Alice is given an input $x \in X$ and Bob is given an input $y \in Y$. The *deterministic communication complexity* of function f is denoted by $D(f)$.

Lemma 7 ([16]). *Alice and Bob each hold an n length string, $x, y \in \{a, b\}^n$, the equality function, $EQ(x, y)$, is defined to be 1 if $x = y$ and 0 otherwise, then*

$$D(EQ) = n + 1. \tag{5}$$

3 State succinctness of 2QCFA on promise problems

In this section, we will give an infinite family of promise problems which can be solved by 2QCFA with one-sided error ϵ with constant numbers of quantum and classical states.

A *promise problem* is a pair $A = (A_{yes}, A_{no})$, where $A_{yes}, A_{no} \subset \Sigma^*$ are sets of strings satisfying $A_{yes} \cap A_{no} = \emptyset$ [30]. Languages may be viewed as promise problems that obey the additional constraint $A_{yes} \cup A_{no} = \Sigma^*$. For an alphabet Σ and any fix $m \in \mathbb{Z}^+$, let $A_{yes}^{meq} = \{w \in \{a, b\}^* | w = a^m b^m\}$ and $A_{no}^{meq} = \{w \in \{a, b\}^* | w \neq a^m b^m \text{ and } |w| \geq m\}$. We

will prove that promise problems $A^{meq} = (A_{yes}^{meq}, A_{no}^{meq})$ can be solved by 2QCFA with one-sided error ϵ with constant numbers of quantum and classical states, whereas the sizes of the corresponding DFA, 2DFA and 2PFA grow without bound.

In order to prove promise problem A^{meq} can be solved by 2QCFA. We first prove a simple promise problem can be solved by 2QCFA. For an alphabet Σ and any fix $m \in \mathbb{Z}^+$, let $A_{yes}^m = \{w \in \Sigma^* \mid |w| = m\}$ and $A_{no}^m = \{w \in \Sigma^* \mid |w| \geq m/2\}$. We will prove that there is a 2QCFA that can solve promise problem $A^m = (A_{yes}^m, A_{no}^m)$ with constant numbers of quantum and classical states. The language $L^m = \{w \in \Sigma^* \mid |w| = m\}$ was showed to be recognized by a 6-state *one way quantum finite automata with restart* ($1QFA^\circ$) with one-sided error ϵ in exponential expected time by Yakaryilmaz and Cem Say [31]. In the very paper, Yakaryilmaz mentioned that $1QFA^\circ$ can be simulated by 2QCFA easily. However, in following theorem we will prove promise problem A^m can be solved by a 2QCFA with one-sided error ϵ in polynomial expected time.

Theorem 8. *For any fix $m \in \mathbb{Z}^+$ and any $\epsilon > 0$, there exists a 2QCFA \mathcal{A}^m which accepts any $w \in A_{yes}^m$ with certainty, and rejects any $w \in A_{no}^m$ with probability at least $1 - \epsilon$, where $QS(\mathcal{A}^m)$ and $CS(\mathcal{A}^m)$ are constant numbers. Furthermore, we have $T(\mathcal{A}^m) \in \mathbf{O}(n^4)$, where $n = |w|$.*

Proof. The main idea is as follows: we consider a 2QCFA \mathcal{A}^m with 2 quantum states $|q_0\rangle$ and $|q_1\rangle$. \mathcal{A}^m starts with the quantum state $|q_0\rangle$. When \mathcal{A}^m reads the left end-marker ϕ , the state is rotated by angle $\sqrt{2}m\pi$ and every time when \mathcal{A}^m reads a symbol $\sigma \in \Sigma^*$, the state is rotated by angle $-\alpha = -\sqrt{2}\pi$ (notice that $\sqrt{2}m\pi = m\alpha$). When the right end-marker $\$$ is reached, \mathcal{A}^m measures the state. If it is $|q_1\rangle$, the input string w is rejected. Otherwise, the process is repeated.

We now describe a 2QCFA \mathcal{A}^m as described in Figure 1 with 2 quantum states $\{|q_0\rangle, |q_1\rangle\}$, of which $|q_0\rangle$ is the initial state. \mathcal{A}^m has two unitary operators: $U_\phi, U_{-\alpha}$, which can be described as follows:

$U_\phi q_0\rangle = \cos m\alpha q_0\rangle + \sin m\alpha q_1\rangle$	$U_{-\alpha} q_0\rangle = \cos \alpha q_0\rangle - \sin \alpha q_1\rangle$
$U_\phi q_1\rangle = -\sin m\alpha q_0\rangle + \cos m\alpha q_1\rangle$	$U_{-\alpha} q_1\rangle = \sin \alpha q_0\rangle + \cos \alpha q_1\rangle$

Lemma 9. *If the input $w \in A_{yes}^m$, then the quantum state of \mathcal{A}^m will evolve into $|q_0\rangle$ after loop 2 with certainty.*

Proof. If $w \in A_{yes}^m$, then $|w| = m$. The quantum state after loop 2 can be described as follows:

$$|q\rangle = (U_{-\alpha})^m U_\phi |q_0\rangle = \begin{pmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{pmatrix}^m \begin{pmatrix} \cos m\alpha & -\sin m\alpha \\ \sin m\alpha & \cos m\alpha \end{pmatrix} |q_0\rangle \quad (6)$$

Repeat the following ad infinitum:

1. Set the quantum state to $|q_0\rangle$ and reads the left end-marker \clubsuit , perform U_\clubsuit on the quantum state.
2. While the currently scanned symbol is not right end-marker $\$$, do the following:
 - (2-1). Every time scan a symbol $\sigma \in \Sigma$, perform $U_{-\alpha}$ on the quantum state.
 - (2-2). Move the tape head one square to the right.
3. Measure the quantum state. If the result is not $|q_0\rangle$, reject.
4. Repeat the following subroutine two times:
 - (4-1). Move the tape head to the first input symbol.
 - (4-2). Move the tape head one square to the right.
 - (4-3). While the currently scanned symbol is not \clubsuit or $\$$, do the following:
 Simulate a coin flip. If the result is “head”, move right. Otherwise, move left.
5. If both times the process ends at the right end-marker $\$$, do:
 Simulate k coin-flips. If all results are “heads”, accept.

Figure 1: 2QCFA algorithm for A^m

$$= \begin{pmatrix} \cos m\alpha & \sin m\alpha \\ -\sin m\alpha & \cos m\alpha \end{pmatrix} \begin{pmatrix} \cos m\alpha & -\sin m\alpha \\ \sin m\alpha & \cos m\alpha \end{pmatrix} |q_0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} |q_0\rangle = |q_0\rangle. \quad (7)$$

□

Lemma 10. *If the input $w \in A_{no}^m$ with $|w| = n$, then \mathcal{A}^m rejects after step 3 with probability at least $1/(2(m-n)^2 + 1)$.*

Proof. Starting with state $|q_0\rangle$, \mathcal{A}^m changes its quantum state to $|q\rangle = (U_{-\alpha})^n U_\clubsuit |q_0\rangle$ after loop 2, the quantum state can be described as follows:

$$|q\rangle = (U_{-\alpha})^n U_\clubsuit |q_0\rangle = \begin{pmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{pmatrix}^n \begin{pmatrix} \cos m\alpha & -\sin m\alpha \\ \sin m\alpha & \cos m\alpha \end{pmatrix} |q_0\rangle \quad (8)$$

$$= \begin{pmatrix} \cos n\alpha & \sin n\alpha \\ -\sin n\alpha & \cos n\alpha \end{pmatrix} \begin{pmatrix} \cos m\alpha & -\sin m\alpha \\ \sin m\alpha & \cos m\alpha \end{pmatrix} |q_0\rangle \quad (9)$$

$$= \begin{pmatrix} \cos(m+n)\alpha & \sin(m-n)\alpha \\ \sin(m-n)\alpha & \cos(m+n)\alpha \end{pmatrix} |q_0\rangle = \cos((m-n)\alpha) |q_0\rangle + \sin((m-n)\alpha) |q_1\rangle. \quad (10)$$

The probability of observing $|q_1\rangle$ is $\sin^2(\sqrt{2}(m-n)\pi)$ in step 3. Without loss of generality, we assume that $m-n > 0$. Let l be the closest integer to $\sqrt{2}(m-n)$. If $\sqrt{2}(m-n) > l$, then $2(m-n)^2 > l^2$. So we get $2(m-n)^2 - 1 \geq l^2$ and $l \leq \sqrt{2(m-n)^2 - 1}$. We have

$$\sqrt{2}(m-n) - l \geq \sqrt{2}(m-n) - \sqrt{2(m-n)^2 - 1} \quad (11)$$

$$= \frac{(\sqrt{2}(m-n) - \sqrt{2(m-n)^2 - 1})(\sqrt{2}(m-n) + \sqrt{2(m-n)^2 - 1})}{\sqrt{2}(m-n) + \sqrt{2(m-n)^2 - 1}} \quad (12)$$

$$= \frac{1}{\sqrt{2}(m-n) + \sqrt{2(m-n)^2 - 1}} > \frac{1}{2\sqrt{2}(m-n)}. \quad (13)$$

Because l is the closest integer to $\sqrt{2}(m-n)$, we have $0 < \sqrt{2}(m-n) - l < 1/2$. Let $f(x) = \sin(x\pi) - 2x$. We have $f''(x) = -\pi^2 \sin(x\pi) \leq 0$ when $x \in [0, 1/2]$. That is to say, $f(x)$ is concave in $[0, 1/2]$, and we have $f(0) = f(1/2) = 0$. So for any $x \in [0, 1/2]$, it holds that $f(x) \geq 0$, that is, $\sin(x\pi) \geq 2x$. Therefore, we have

$$\sin^2(\sqrt{2}(m-n)\pi) = \sin^2((\sqrt{2}(m-n) - l)\pi) \quad (14)$$

$$\geq (2(\sqrt{2}(m-n) - l))^2 = 4(\sqrt{2}(m-n) - l)^2 \quad (15)$$

$$> 4\left(\frac{1}{2\sqrt{2}(m-n)}\right)^2 = \frac{1}{2(m-n)^2} > \frac{1}{2(m-n)^2 + 1}. \quad (16)$$

If $\sqrt{2}(m-n) < l$, then $2(m-n)^2 < l^2$. So we get $2(m-n)^2 + 1 \leq l^2$ and $l \geq \sqrt{2(m-n)^2 + 1}$. We have

$$\sqrt{2}(m-n) - l \leq \sqrt{2}(m-n) - \sqrt{2(m-n)^2 + 1} \quad (17)$$

$$= \frac{(\sqrt{2}(m-n) - \sqrt{2(m-n)^2 + 1})(\sqrt{2}(m-n) + \sqrt{2(m-n)^2 + 1})}{\sqrt{2}(m-n) + \sqrt{2(m-n)^2 + 1}} \quad (18)$$

$$= \frac{-1}{\sqrt{2}(m-n) + \sqrt{2(m-n)^2 + 1}} < \frac{-1}{2\sqrt{2(m-n)^2 + 1}}. \quad (19)$$

It follows that

$$l - \sqrt{2}(m-n) > \frac{1}{2\sqrt{2(m-n)^2 + 1}}. \quad (20)$$

Because l is the closest integer to $\sqrt{2}(m-n)$, we have $0 < l - \sqrt{2}(m-n) < 1/2$. Therefore, we have

$$\sin^2(\sqrt{2}(m-n)\pi) = \sin^2((\sqrt{2}(m-n) - l)\pi) \quad (21)$$

$$= \sin^2((l - \sqrt{2}(m-n))\pi) \geq (2(l - \sqrt{2}(m-n)))^2 \quad (22)$$

$$= 4(l - \sqrt{2}(m-n))^2 > 4\left(\frac{1}{2\sqrt{2(m-n)^2 + 1}}\right)^2 = \frac{1}{2(m-n)^2 + 1}. \quad (23)$$

So the lemma has been proved. \square

Simulation of a coin flip in loops **4** and **5** is a necessary component in the above algorithm. We will show that coin-flips can be simulated by 2QCFA using two quantum states $|q_0\rangle$ and $|q_1\rangle$.

Lemma 11. *A coin flip in the algorithm can be simulated by 2QCFA \mathcal{A}^m using two quantum states $|q_0\rangle$ and $|q_1\rangle$.*

Proof. A projective measurement $M = \{P_0, P_1\}$ is defined by

$$P_0 = |q_0\rangle\langle q_0|, P_1 = |q_1\rangle\langle q_1|. \quad (24)$$

The results 0 and 1 represent the “tail” and “head” of a coin flip, respectively. A unitary operator U is given by

$$U = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}. \quad (25)$$

The unitary operator U changes the state as follows:

$$|q_0\rangle \rightarrow |\psi\rangle = \frac{1}{\sqrt{2}}(|q_0\rangle + |q_1\rangle), \quad |q_1\rangle \rightarrow |\phi\rangle = \frac{1}{\sqrt{2}}(|q_0\rangle - |q_1\rangle). \quad (26)$$

Suppose now that the machine starts with the state $|q_0\rangle$, changes its state by U , and then measures the state with M . Then we will get the result 0 or 1 with probability $\frac{1}{2}$. This is similar to a coin flip process. \square

Lemma 12. [3] *Let the length of the input string $|w| = n$, then every execution of loops 4 and 5 leads to acceptance with probability $1/2^k(n+1)^2$.*

Proof. Loop 4 is two times of random walk starting at location 1 and ending at location 0 (the left end-marker ϕ) or at location $n+1$ (the right end-marker $\$$). It can be known from probability theory that the probability of reaching the location $n+1$ is $1/(n+1)$ (see Chapter 14.2 in [12]). Repeating it twice and flipping k coins, we get the probability $1/2^k(n+1)^2$. \square

Let $k = 1 + \lceil \log_2 1/\varepsilon \rceil$, then $\varepsilon \geq 1/2^{k-1}$. Assume that $|w| = n$, if $w \in A_{yes}^m$, loop 2 always changes $|q_0\rangle$ to $|q_0\rangle$, and \mathcal{A}^m never rejects after the measurement in step 3. After loops 4 and 5, the probability of \mathcal{A}^m accepting w is $1/2^k(n+1)^2$. Repeating loops 4 and 5 for cn^2 times, the accepting probability is

$$Pr[\mathcal{A}^m \text{ accepts } w] = 1 - (1 - \frac{1}{2^k(n+1)^2})^{cn^2}, \quad (27)$$

and this can be made arbitrarily close to 1 by selecting constant c appropriately.

Otherwise, if $|w| \in A_{no}^m$, \mathcal{A}^m rejects after loop 2 and step 3 with probability

$$P_r > \frac{1}{2(m-n)^2 + 1} \quad (28)$$

according to Lemma 10. \mathcal{A}^m accepts after loops 4 and 5 with probability

$$P_a = 1/2^k(n+1)^2 \leq \varepsilon/2(n+1)^2. \quad (29)$$

If we repeat the whole algorithm indefinitely, the probability of \mathcal{M} rejecting input w is

$$\Pr[\mathcal{A}^m \text{ rejects } w] = \sum_{i \geq 0} (1 - P_a)^i (1 - P_r)^i P_r \quad (30)$$

$$= \frac{P_r}{P_a + P_r - P_a P_r} > \frac{P_r}{P_a + P_r} \quad (31)$$

$$> \frac{1/(2(n-m)^2 + 1)}{\varepsilon/2(n+1)^2 + 1/(2(n-m)^2 + 1)} \quad (32)$$

$$= \frac{(n+1^2)/(2(n-m)^2 + 1)}{\varepsilon/2 + (n+1)^2/(2(n-m)^2 + 1)} \quad (33)$$

Let $f(x) = \frac{x}{\varepsilon/2+x} = 1 - \frac{\varepsilon}{(\varepsilon+2x)}$, then $f(x)$ is monotonous increasing in $(0, +\infty)$. By assumption, we have $n = |w| \geq m/2$. So we have $(n+1^2)/(2(n-m)^2 + 1) > 1/2$. Therefore, we have

$$> \frac{1/2}{1/2 + \varepsilon/2} = \frac{1}{1 + \varepsilon} > 1 - \varepsilon. \quad (34)$$

If we assume that the length of the input $|w| = n$, then step **1** takes $\mathbf{O}(1)$ time, loop **2** and step **3** take $\mathbf{O}(n)$ time, and loops **4** and **5** take $\mathbf{O}(n^2)$ time. The expected number of repeating the algorithm is $\mathbf{O}(n^2)$. Hence, the expected running time of \mathcal{A}^m is $\mathbf{O}(n^4)$. Obviously, the 2QCFA \mathcal{A}^m has two quantum states and constant classical states.

□

Theorem 13. *For any $m \in \mathbb{Z}^+$ and any $\epsilon > 0$, there exists a 2QCFA \mathcal{A}^{meq} which accepts any $w \in A_{yes}^{meq}$ with certainty, and rejects any $w \in A_{no}^{meq}$ with probability at least $1 - \epsilon$, where $QS(\mathcal{A}^{meq})$ and $CS(\mathcal{A}^{meq})$ are constant numbers. Furthermore, we have $T(\mathcal{A}^{meq}) \in \mathbf{O}(n^4)$ where $|w| = n$.*

Proof. Let the alphabet $\Sigma = \{a, b\}$, obviously, $A^{meq} = L^{eq} \cap A^{2m}$. According to Lemma 1, for any $\epsilon_1 > 0$, there is a 2QCFA \mathcal{A}_1 recognizes L^{eq} with one-sided error ϵ_1 , and $QS(\mathcal{A}_1) = 2$, $CS(\mathcal{A}_1) = k_1$ and $T(\mathcal{A}_1) \in \mathbf{O}(n^4)$ where k_1 is a constant and n is the length of the input. According to Theorem 8, for any $\epsilon_2 > 0$, there is a 2QCFA \mathcal{A}_2 solves A^{2m} with one-sided error ϵ_2 , and $QS(\mathcal{A}_2) = 2$, $CS(\mathcal{A}_2) = k_2$ and $T(\mathcal{A}_2) \in \mathbf{O}(n^4)$ where k_2 is a constant and n is the length of the input. For any $\epsilon > 0$, let $\epsilon_1 = \epsilon/2$ and $\epsilon_2 = \epsilon/2$, according to Lemma 2, there is a 2QCFA \mathcal{A} solves $L^{eq} \cap A^{2m}$ with one-sided error ϵ , where $QS(\mathcal{A}) = QS(\mathcal{A}_1) + QS(\mathcal{A}_2) = 4$, $CS(\mathcal{A}) = CS(\mathcal{A}_1) + CS(\mathcal{A}_2) + QS(\mathcal{A}_1) = k_1 + k_2 + 2$ and $T(\mathcal{A}) = T(\mathcal{A}_1) + T(\mathcal{A}_2) \in \mathbf{O}(n^4)$. Hence, the theorem has been proved. □

Remark 2. Actually, L_1 and L_2 must be languages in Lemma 2. But in Theorem 13, we used a promise problem A^{2m} . It is easy to show that Lemma 2 still holds for promise problem A^{2m} and L^{eq} . We used Lemma 2 to prove Theorem 13 in this section. However, we can prove Theorem 13 directly.

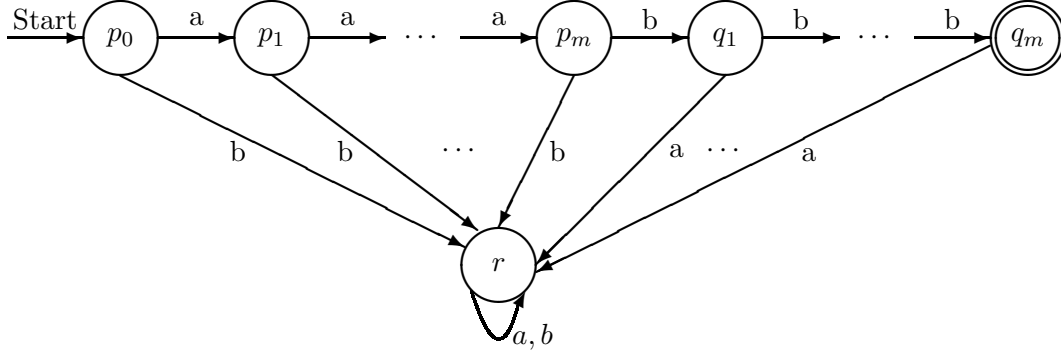


Figure 2: DFA \mathcal{A} solving A^{meq}

Obviously, there exists a DFA depicted in Figure 2 that solves A^{meq} with $2m+2$ states..

Theorem 14. *For any fix $m \in \mathbb{Z}^+$, any DFA solving promise problem A^{meq} has at least $2m + 2$ states.*

Proof. Let string set $W = \{a^0, a^1, \dots, a^m, a^m b^1, a^m b^2, \dots, a^m b^m\}$, where a^0 is the empty string. Obviously, for any two different strings $w_i, w_j \in W$, we have $|w_i| \neq |w_j|$, and if $|w_i| < |w_j|$, then w_i is a prefix of w_j . For any string $x \in \Sigma^*$ and any $\sigma \in \Sigma$, let $\hat{\delta}(s, \sigma x) = \hat{\delta}(\delta(s, \sigma), x)$; if $|x| = 0$, $\hat{\delta}(s, x) = s$ [14]. Assume that a n -state DFA \mathcal{A} solves promise problem A^{meq} . We show that n cannot be less than $2m + 2$.

Assume that s_0 is initial state of \mathcal{A} , if there are two different strings $w_i, w_j \in W$ satisfy that $\hat{\delta}(s_0, w_i) = \hat{\delta}(s_0, w_j)$. Without lose of generality, we assume that w_i is a prefix of w_j , so there is a string x satisfies $w_j = w_i x$, where $|x| \neq 0$. Let $\hat{\delta}(s_0, w_i) = s$, we have $\hat{\delta}(s, x^*) = s$. Because w_i is a prefix of $a^m b^m$, there exists a string y satisfies that $\hat{\delta}(s_0, w_i y) = \hat{\delta}(s, y) = s_{acc}$, where s_{acc} is an accepting state. It follow $\hat{\delta}(s_0, w_i x^* y) = s_{acc}$. Therefore, there is some $k \in \mathbb{Z}^+$ satisfy that $\hat{\delta}(s_0, w_i x^k y) = s_{acc}$ and $w_i x^k y \in A_{no}^{meq}$, which is a contradiction. Hence, for any two different strings $w_i, w_j \in W$ satisfy that $\hat{\delta}(s_0, w_i) \neq \hat{\delta}(s_0, w_j)$.

For any $w_i \in W$, $\hat{\delta}(s_0, w_i)$ are reachable state (i.e., there exists a string z satisfies that $\hat{\delta}(\hat{\delta}(s_0, w_i), z)$ is an accepting state). There must be at least a not reachable state, for example, $\hat{\delta}(s_0, a^m b^{m+1})$. There is $2m + 1$ elements in set W and at least one not reachable state. So any DFA solving promise problem A^{meq} has at least $2m + 2$ states. □

Theorem 15. *For any fix $m \in \mathbb{Z}^+$, any 2DFA, 2NFA and polynomial expected running time recognizing L^{mtwin} have at least $\sqrt{\log m}$, $\sqrt{\log m}$ and $\sqrt[3]{(\log m)/b}$ states, where b is a constant number.*

Proof. Assume that a n_1 -state 2DFA \mathcal{A} solves promise problem A^{meq} . It is easy to prove

that $n_1 \geq 3$. According to Lemma 3, there is a DFA solves promise problem A^{meq} with $(n_1 + 1)^{n_1+1}$ states. According to Theorem 14, we have

$$(n_1 + 1)^{n_1+1} \geq 2m + 2 \Rightarrow (n_1 + 1) \log(n_1 + 1) > \log m + 1. \quad (35)$$

Because $n_1 \geq 3$, we get

$$n_1^2 > (n_1 + 1) \log(n_1 + 1) > \log m \Rightarrow n > \sqrt{\log m}. \quad (36)$$

Assume that a n_2 -state 2NFA \mathcal{A} solves promise problem A^{meq} . According to Lemma 4, there is a DFA solves promise problem A^{meq} with $2^{(n_2-1)^2+n_2}$ states. According to Theorem 14, we have

$$2^{(n_2-1)^2+n_2} \geq 2m + 2 \Rightarrow (n_2 - 1)^2 + n_2 > \log m + 1 \quad (37)$$

$$\Rightarrow n_2^2 > \log m \Rightarrow n_2 > \sqrt{\log m}. \quad (38)$$

Assume that a n_3 -state 2PFA \mathcal{A} solves promise problem A^{meq} with bounded error $\epsilon < 1/2$ and within polynomial expected running time. According to Lemma 5, there is a DFA solves promise problem A^{meq} with $n_3^{bn_3^2}$ states, where $b > 0$ is a constant. According to Theorem 14, we have

$$n_3^{bn_3^2} \geq 2m + 2 \Rightarrow bn_3^2 \log n_3 > \log m \quad (39)$$

$$\Rightarrow n_3^3 > (\log m)/b \Rightarrow n_3 > \sqrt[3]{(\log m)/b}. \quad (40)$$

□

4 State succinctness of 2QCFA on languages

For an alphabet Σ and any fix $m \in \mathbb{Z}^+$, let $L^{mtwin} = \{wcw | w \in \{a, b\}^*, |w| = m, \Sigma = \{a, b, c\}\}$. For any $\epsilon > 0$, we will prove that L^{mtwin} can be recognized by 2QCFA with constant numbers of quantum and classical states with one-sided error ϵ in exponential expected running time. The language $L^{twin} = \{wcw | w \in \{a, b\}^*, \Sigma = \{a, b, c\}\}$ was mentioned to be recognized by 2QCFA in theory by Yakaryilmaz and Cem Say [31]. However, Yakaryilmaz and Cem Say did not give the details of the 2QCFA. In the following, we will show the details.

Theorem 16. *For any $\epsilon > 0$, there exists a 2QCFA \mathcal{A} which accepts any $w \in L^{twin}$ with certainty, rejects any $w \notin L^{twin}$ with probability at least $1 - \epsilon$, and halts in exponential expected time, where $QS(\mathcal{A})=3$ and $CS(\mathcal{A})$ is constant number.*

Proof. In order to prove Theorem 16, we consider 3×3 matrixes U_a and U_b defined as follows:

$$A = \begin{pmatrix} 4 & 3 & 0 \\ -3 & 4 & 0 \\ 0 & 0 & 5 \end{pmatrix}, B = \begin{pmatrix} 4 & 0 & 3 \\ 0 & 5 & 0 \\ -3 & 0 & 4 \end{pmatrix}. \quad (41)$$

Check whether the input is of the form xcy ($x, y \in \Sigma^*$). If not, reject.

Otherwise, repeat the following ad infinitum:

1. Move the tape head to the first input symbol and set the quantum state to $|q_0\rangle$.
2. While the currently scanned symbol is not c , do the following:
 - (2-1). Perform U_σ on the quantum state, for σ denoting the currently scanned symbol.
 - (2-2). Move the tape head one square to the right.
3. Move the tape head to last input symbol.
4. While the currently scanned symbol is not c , do the following:
 - (4-1). Perform U_σ^{-1} on the quantum state, for σ denoting the currently scanned symbol.
 - (4-2). Move the tape head one square to the left.
5. Measure the quantum state. If the result is not $|q_0\rangle$, reject.
6. Move the tape head to last input symbol and set $b=0$.
7. While the currently scanned symbol is not ϕ , do the following:
 - (7-1). Simulate k coin-flips. Set $b = 1$ in case all results are not “heads”.
 - (7-2). Move the tape head one square to the left.
8. If $b=0$, accept.

Figure 3: 2QCFA algorithm for L^{twin}

We now describe a 2QCFA \mathcal{A} as described in Figure 3 with 3 quantum states $\{|q_0\rangle, |q_1\rangle, |q_2\rangle\}$, of which $|q_0\rangle$ is the initial state. \mathcal{A} has two unitary operators $U_a = \frac{1}{5}A$ and $U_b = \frac{1}{5}B$ given in Eq. (41). They can also be described as follows:

$U_a q_0\rangle = \frac{4}{5} q_0\rangle - \frac{3}{5} q_1\rangle$	$U_b q_0\rangle = \frac{4}{5} q_0\rangle - \frac{3}{5} q_2\rangle$
$U_a q_1\rangle = \frac{3}{5} q_0\rangle + \frac{4}{5} q_1\rangle$	$U_b q_1\rangle = q_1\rangle$
$U_a q_2\rangle = q_2\rangle$	$U_b q_2\rangle = \frac{3}{5} q_0\rangle + \frac{4}{5} q_2\rangle$

We pick up some definitions in [3] before we prove the Theorem. Let $u \in \mathbb{Z}^3$, we use $u[i]$ ($i = 1, 2, 3$) to denote the i th entry of u . We define a function $f : \mathbb{Z}^3 \rightarrow \mathbb{Z}$ as

$$f(u) = 4u[1] + 3u[2] + 3u[3] \quad (42)$$

for each $u \in \mathbb{Z}^3$, and we define a set $K \subseteq \mathbb{Z}^3$ as

$$K = \{u \in \mathbb{Z}^3 : u[1] \not\equiv 0 \pmod{5}, f(u) \not\equiv 0 \pmod{5}, \text{ and } u[2] \cdot u[3] \equiv 0 \pmod{5}\} \quad (43)$$

Lemma 17 ([3]). *If $u \in K$, then $Au \in K$ and $Bu \in K$.*

Lemma 18 ([3]). *If $u \in \mathbb{Z}^3$ satisfy $u = Av = Bw$ for $v, w \in \mathbb{Z}^3$, then $u \notin K$.*

Lemma 19. *If $u \in K$, there does not exist a $l \in \mathbb{Z}^+$ satisfies that $Xu = \pm 5^l(1, 0, 0)^T$, where $X \in \{A, B\}$.*

Proof. Suppose there is a $l \in \mathbb{Z}^+$ satisfies that $Xu = \pm 5^l(1, 0, 0)^T$. Assume that $X = A$ (the proof for $X = B$ is similar), then we have

$$Xu = Au = \begin{pmatrix} 4 & 3 & 0 \\ -3 & 4 & 0 \\ 0 & 0 & 5 \end{pmatrix} \begin{pmatrix} u[1] \\ u[2] \\ u[3] \end{pmatrix} = \begin{pmatrix} 4u[1] + 3u[2] \\ -3u[1] + 4u[2] \\ 5u[3] \end{pmatrix} = \pm \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} 5^l \quad (44)$$

$$\Rightarrow \begin{pmatrix} u[1] \\ u[2] \\ u[3] \end{pmatrix} = \pm \begin{pmatrix} 4 \cdot 5^{l-2} \\ 3 \cdot 5^{l-2} \\ 0 \end{pmatrix}. \quad (45)$$

Since $4u[1] + 3u[2] + 3u[3] = \pm(16 \cdot 5^{l-2} + 9 \cdot 5^{l-2}) = \pm 5^l$, we conclude $f(u) \equiv 0 \pmod{5}$. We get $u \notin K$, contradicts the fact that $u \in K$. Hence, the Lemma has been proved. \square

Corollary 20. *Let*

$$u = X_k \cdots X_1(1, 0, 0)^T, \quad (46)$$

where $X_i \in \{A, B\}$, for every $l \in \mathbb{Z}^+$ satisfies that $u \neq \pm 5^l(1, 0, 0)^T$.

Proof. Clearly, $(1, 0, 0)^T \in K$. According to Lemma 17, $X_{k-1} \cdots X_1(1, 0, 0)^T \in K$. According to Lemma 19, there does not exist $l \in \mathbb{Z}^+$ satisfies that $u = \pm 5^l(1, 0, 0)^T$. \square

Lemma 21. *Let*

$$u = Y_1^{-1} \cdots Y_k^{-1}(1, 0, 0)^T, \quad (47)$$

where $Y_i \in \{A, B\}$, for every $l \in \mathbb{Z}^+$ satisfies that $u \neq \pm \frac{1}{5^l}(1, 0, 0)^T$.

Proof. Assume that there is a $l \in \mathbb{Z}^+$ satisfies that $u = Y_1^{-1} \cdots Y_k^{-1}(1, 0, 0)^T = \pm \frac{1}{5^l}(1, 0, 0)^T$, then we get $Y_k \cdots Y_1(1, 0, 0)^T = \pm 5^l(1, 0, 0)^T$. According to Corollary 20, such l does not exist. \square

Lemma 22. *Let*

$$u = (5Y_1^{-1}) \cdots (5Y_m^{-1})(5^{-1}X_n) \cdots (5^{-1}X_1)(1, 0, 0)^T, \quad (48)$$

where $X_j, Y_j \in \{A, B\}$. If $m = n$ and $X_j = Y_j$ for $1 \leq j \leq n$, then $u[2]^2 + u[3]^2 = 0$. Otherwise, $u[2]^2 + u[3]^2 > 5^{-(n+m)}$.

Proof. If $m = n$ and $X_j = Y_j$ for $1 \leq j \leq n$, then we have

$$u = Y_1^{-1} \cdots Y_n^{-1} X_n \cdots X_1(1, 0, 0)^T = (1, 0, 0)^T, \quad (49)$$

and thus $u[2]^2 + u[3]^2 = 0$.

Otherwise, note that $\|u\| = 1$, since $5^{-1}X_j$ and $5Y_j^{-1}$ are unitary for each j , and further note that $5^{(n+m)}u$ is integer valued. It is therefore suffices to prove $u \neq \pm(1, 0, 0)^T$, since $|u[1]| < 1$ implies $|u[1]| \leq 1 - 5^{-(n+m)}$, and therefore

$$u[2]^2 + u[3]^2 = 1 - u[1]^2 \geq 1 - (1 - 5^{-(n+m)})^2 > 5^{-(n+m)}. \quad (50)$$

We first prove the case that $n \geq m$. If $X_{n-j} = Y_{m-j}$ for $0 \leq j \leq m-1$, then

$$u = (5Y_1^{-1}) \cdots (5Y_m^{-1})(5^{-1}X_n) \cdots (5^{-1}X_1)(1, 0, 0)^T = 5^{-(n-m)}X_{n-m} \cdots X_1(1, 0, 0)^T. \quad (51)$$

According to Corollary 20, for every $l \in \mathbb{Z}^+$,

$$u = 5^{-(n-m)}X_{n-m} \cdots X_1(1, 0, 0)^T \neq \pm 5^{-(n-m)}5^l(1, 0, 0)^T. \quad (52)$$

Let $l = n - m$, we conclude that $u \neq \pm(1, 0, 0)^T$.

Next suppose there exist $i < m$ such that $X_{n-i} \neq Y_{m-i}$. Let k be the smallest index such that $X_{n-k} \neq Y_{m-k}$, and without loss of generality suppose $X_{n-k} = A, Y_{m-k} = B$. Since $X_{n-j} = Y_{m-j}$ for $j < k$, we have

$$u = (5Y_1^{-1}) \cdots (5Y_m^{-1})(5^{-1}X_n) \cdots (5^{-1}X_1)(1, 0, 0)^T = 5^{-(n-m)}Y_1^{-1} \cdots Y_{m-k}^{-1}X_{n-k} \cdots X_1(1, 0, 0)^T. \quad (53)$$

Suppose $u = (1, 0, 0)^T$, we get

$$u = 5^{-(n-m)}Y_1^{-1} \cdots Y_{m-k}^{-1}X_{n-k} \cdots X_1(1, 0, 0)^T = (1, 0, 0)^T \quad (54)$$

$$\Rightarrow X_{n-k} \cdots X_1(1, 0, 0)^T = 5^{(n-m)}Y_{m-k} \cdots Y_1(1, 0, 0)^T = Y_{m-k} \cdots Y_1 5^{(n-m)}(1, 0, 0)^T \quad (55)$$

Obviously, $(1, 0, 0)^T \in K$ and $5^{(n-m)}(1, 0, 0)^T \in K$. Let $v = X_{n-k-1} \cdots X_1(1, 0, 0)^T$ and $w = Y_{m-k-1} \cdots Y_1 5^{(n-m)}(1, 0, 0)^T$, according to Lemma 17, we have $v, w \in K$, $X_{n-k}v = Av \in K$, and $Y_{m-k}w = Bw \in K$. By Lemma 18 this implies $Av \neq Bw$, which contradicts the Equation 55. We conclude $u \neq (1, 0, 0)^T$. By similar reasoning, $u \neq -(1, 0, 0)^T$.

Now we prove the case that $n < m$. If $X_{n-j} = Y_{m-j}$ for $0 \leq j \leq n-1$, then

$$u = (5Y_1^{-1}) \cdots (5Y_m^{-1})(5^{-1}X_n) \cdots (5^{-1}X_1)(1, 0, 0)^T = 5^{m-n}Y_1^{-1} \cdots Y_{m-n}^{-1}(1, 0, 0)^T. \quad (56)$$

According to Lemma 21, for every $l \in \mathbb{Z}^+$,

$$u = 5^{m-n}Y_1^{-1} \cdots Y_{m-n}^{-1}(1, 0, 0)^T \neq \pm 5^{m-n}5^{-l}(1, 0, 0)^T. \quad (57)$$

Let $l = m - n$, we conclude that $u \neq \pm(1, 0, 0)^T$.

Next suppose there exist $j < n$ such that $X_{n-j} \neq Y_{m-j}$. Let k be the smallest index such that $X_{n-k} \neq Y_{m-k}$, by similar reasoning as the case $n \geq m$, $u \neq \pm(1, 0, 0)^T$.

□

If the input w is not of the form xcy , \mathcal{A} rejects w immediately.

Lemma 23. *If the input $w = xcy$ satisfies $x = y$, then the quantum state of \mathcal{A} will evolve into $|q_0\rangle$ after loop 4 with certainty.*

Proof. We assume that $x = x_1x_2\cdots x_l$, we have $y = x$, that is $y_i = x_i$ (for $i = 1, 2, \dots, l$). Starting with state $|q_0\rangle$, \mathcal{A} changes its quantum state to $|\psi\rangle$ after loop 4, where

$$|\psi\rangle = U_{y_1}^{-1}U_{y_2}^{-1}\cdots U_{y_l}^{-1}U_{x_l}\cdots U_{x_2}U_{x_1}|q_0\rangle = U_{x_1}^{-1}U_{x_2}^{-1}\cdots U_{x_l}^{-1}U_{x_l}\cdots U_{x_2}U_{x_1}|q_0\rangle = |q_0\rangle. \quad (58)$$

□

Lemma 24. *If the input $w = xcy$ satisfies $x \neq y$, then \mathcal{A} rejects after step 5 with probability at least $5^{-(m+n)}$.*

Proof. We assume that $x = x_1x_2\cdots x_n$, $y = y_1y_2\cdots y_m$. Starting with state $|q_0\rangle$, \mathcal{A} changes its quantum state to $|\psi\rangle$ after loop 4, where

$$|\psi\rangle = U_{y_1}^{-1}U_{y_2}^{-1}\cdots U_{y_m}^{-1}U_{x_n}\cdots U_{x_2}U_{x_1}|q_0\rangle. \quad (59)$$

Write $|\psi\rangle = \beta_0|q_0\rangle + \beta_1|q_1\rangle + \beta_2|q_2\rangle$, according to Lemma 22, $\beta_1^2 + \beta_2^2 > 5^{-(n+m)}$. In step 5, the quantum state $|\psi\rangle$ is measured, \mathcal{A} rejects w with probability $p_r = \beta_1^2 + \beta_2^2 > 5^{-(n+m)}$. □

Every execution of step 6, loop 7 and step 8 leads to acceptance with probability $2^{-k(n+m+1)}$.

Let $k \geq \max\{\log 5, -\log \epsilon\}$. Assume the input is of the form $w = xcy$, if $x = y$, 2QCFA \mathcal{A} always changes its quantum state to $|q_0\rangle$ after loop 4, and \mathcal{A} never rejects after the measurement in step 5. After step 6, loop 7 and step 8, the probability of \mathcal{A} accepting w is $2^{-k(n+m+1)}$. Repeating the whole iteration for $c2^{k(n+m+1)}$ times, the accepting probability is

$$Pr[\mathcal{A} \text{ accepts } w] = 1 - (1 - 2^{-k(n+m+1)})^{c2^{k(n+m+1)}}, \quad (60)$$

and this can be made arbitrarily close to 1 by selecting constant c appropriately.

Otherwise, $x \neq y$, \mathcal{A} rejects after step 5 with probability

$$P_r > 5^{-(m+n)} \quad (61)$$

according to Lemma 24. \mathcal{A} accepts after 6, loop 7 and step 8 with probability

$$P_a = 2^{-k(n+m+1)}. \quad (62)$$

If we repeat the whole iteration indefinitely, the probability of \mathcal{A} rejecting input w is

$$Pr[\mathcal{A} \text{ rejects } w] = \sum_{i \geq 0} (1 - P_a)^i (1 - P_r)^i P_r \quad (63)$$

$$= \frac{P_r}{P_a + P_r - P_a P_r} > \frac{P_r}{P_a + P_r} \quad (64)$$

$$> \frac{5^{-(m+n)}}{2^{-k(n+m+1)} + 5^{-(m+n)}} \quad (65)$$

$$> \frac{1}{1 + \varepsilon} > 1 - \varepsilon. \quad (66)$$

If we assume that the input is w , then step **1** takes $\mathbf{O}(1)$ time, loop **2** and step **3** take $\mathbf{O}(|w|)$ time, loops **4** and step **5** take $\mathbf{O}(|w|)$ time, step **6**, loop **7** and step **8** take $\mathbf{O}(|w|)$ time. The expected number of repeating the iteration is $\mathbf{O}(2^{k|w|})$. Hence, the expected running time of \mathcal{A} is $\mathbf{O}(|w|2^{k|w|})$. Obviously, the 2QCFA \mathcal{A} has three quantum states and constant classical states. \square

In Theorem 16, we have proved that L^{twin} can be recognized by 2QCFA. We will show that L^{twin} can not be recognized by 2PFA with bounded error. Thus L^{twin} is another witness of the fact that 2QCFA are more powerful than their classical counterparts 2PFA.

Theorem 25. *There is no 2PFA recognizing L^{twin} with bounded error.*

Proof. Let $A = L^{twin}$ and $B = \overline{L^{twin}} = \Sigma^* \setminus A$. Clearly, for each $m \in I$, there is a set $W_m \subseteq \Sigma^*$ satisfy conditions (1) and (2) of Lemma 6. For every $m \in I$ and every $w, w' \in W_m$ with $w \neq w'$, take $u = \lambda$ (the empty word) and $v = cw$, then $uwv = wcv \in A$ and $uw'v = w'cv \in B$. Thus, the Theorem has been proved. \square

Lemma 26 ([31]). *For any error bound $\epsilon > 0$, there exists a 7-state $1QFA^\circ$ \mathcal{A} which accepts any $w \in L^m$ with certainty, and rejects any $w \notin L^m$ with probability at least $1 - \epsilon$. Moreover, the expected runtime of the \mathcal{A} on w is $\mathbf{O}(2^m|w|)$.*

Remark 3. In Lemma 26, when $w \in L^m$, we have $|w| = m$. Hence the expected runtime $\mathbf{O}(2^m|w|)$ is exponential.

Lemma 27 ([31]). *For any $1QFA^\circ$ \mathcal{A}_1 with n quantum states and expected running time $t(|w|)$, there exists a 2QCFA \mathcal{A}_2 with n quantum states, $\mathbf{O}(n)$ classical states, and expected running time $\mathbf{O}(t(|w|))$, such that \mathcal{A}_2 accepts every input string w with the same probability that \mathcal{A}_1 accepts w .*

Theorem 28. *For any error bound $\epsilon > 0$, there exists a 2QFA \mathcal{A} which accepts any $w \in L^m$ with certainty, and rejects any $w \notin L^m$ with probability at least $1 - \epsilon$. Moreover, $QS(\mathcal{A}) = 7$, $CS(\mathcal{A})$ is a constant number, and the expected runtime of the \mathcal{A} on w is $\mathbf{O}(2^m|w|)$.*

Proof. It follows from Lemma 26 and Lemma 27. \square

Theorem 29. *For any error bound $\epsilon > 0$, there exists a 2QFA \mathcal{A} which accepts any $w \in L^{mtwin}$ with certainty, and rejects any $w \notin L^{mtwin}$ with probability at least $1 - \epsilon$. Moreover, $QS(\mathcal{A})$, $CS(\mathcal{A})$ are constant numbers, and the expected running time of \mathcal{A} on w is $\mathbf{O}(|w|2^{k|w|})$.*

Proof. Let the alphabet $\Sigma = \{a, b, c\}$, obviously, $L^{mtwin} = L^{twin} \cap L^{2m+1}$. According to Theorem 16, for any $\epsilon_1 > 0$, there is a 2QCFA \mathcal{A}_1 recognizes L^{twin} with one-sided error ϵ_1 , and $QS(\mathcal{A}_1) = 3$, $CS(\mathcal{A}_1) = k_1$ and $T(\mathcal{A}_1) \in \mathbf{O}(|w|2^{k|w|})$ where k_1 and k are constant numbers. According to Theorem 28, for any $\epsilon_2 > 0$, there is a 2QCFA \mathcal{A}_2 recognizes L^{2m+1} with one-sided error ϵ_2 , and $QS(\mathcal{A}_2) = 7$, $CS(\mathcal{A}_2) = k_2$ and $T(\mathcal{A}_2) \in \mathbf{O}(2^m|w|)$ where k_2 is a constant. For any $\epsilon > 0$, let $\epsilon_1 = \epsilon/2$ and $\epsilon_2 = \epsilon/2$, according to Lemma 2, there is a 2QCFA \mathcal{A} recognizes $L^{twin} \cap L^{2m+1}$ with one-sided error ϵ , where $QS(\mathcal{A}) = QS(\mathcal{A}_1) + QS(\mathcal{A}_2) = 10$, $CS(\mathcal{A}) = CS(\mathcal{A}_1) + CS(\mathcal{A}_2) + QS(\mathcal{A}_1) = k_1 + k_2 + 3$ and $T(\mathcal{A}) = T(\mathcal{A}_1) + T(\mathcal{A}_2) \in \mathbf{O}(|w|2^{k|w|})$. Hence, the theorem has been proved. \square

For a fix $m \in \mathbb{Z}^+$, L^{mtwin} is finite, and thus there exists an DFA for L^{mtwin} . We may want to know that the numbers of states required in a DFA for language L^{mtwin} . Here, we use lower bounds in the area of *communication complexity* to prove the lower bound of states required in a DFA.

Theorem 30. *For any fix $m \in \mathbb{Z}^+$, any DFA recognizing L^{mtwin} has at least 2^m states.*

Proof. Assume that DFA \mathcal{A} recognizes L^{mtwin} . A protocol for f will work as follows: On input (x, y) (each of length m), let the string $w = xcy$ be the input of DFA \mathcal{A} . Alice simulates the path taken by DFA \mathcal{A} on her input x . She then sends the name of the last state s in this path to Bob, which need $\log(|S|)$ bits, where S is the finite state set of states in DFA \mathcal{A} . Then, Bob simulates DFA \mathcal{A} , starting from state s , on input cy . At last, Bob sends the result to Alice, if w is accepted, sends 1, otherwise 0. All together, they get a simulation of DFA \mathcal{A} on input $w = xcy$. By assumption, if $w = xcy$ is accepted by DFA \mathcal{A} then $EQ(x, y) = 1$ while if w is rejected then $EQ(x, y) = 0$. Therefore, we have $D(EQ) \leq \log(|S|) + 1$. According to Lemma 7, we have

$$D(EQ) = m + 1 \leq \log(|S|) + 1 \quad (67)$$

$$\Rightarrow m \leq \log(|S|) \Rightarrow |S| \geq 2^m. \quad (68)$$

\square

Theorem 31. *For any fix $m \in \mathbb{Z}^+$, any 2DFA, 2NFA and polynomial expected running time recognizing L^{mtwin} have at least \sqrt{m} , \sqrt{m} and $\sqrt[3]{m/b}$ states, where b is a constant number.*

Proof. Assume that a n_1 -state 2DFA \mathcal{A} recognizes L^{mtwin} . It is easy to prove that $n_1 \geq 3$. According to Lemma 3, there is a DFA recognizes L^{mtwin} with $(n_1 + 1)^{n_1 + 1}$ states. According

to Theorem 30, we have

$$(n_1 + 1)^{n_1+1} \geq 2^m \Rightarrow (n_1 + 1) \log(n_1 + 1) \geq m. \quad (69)$$

Because $n \geq 3$, we get

$$n_1^2 > (n_1 + 1) \log(n_1 + 1) > m \Rightarrow n_1 > \sqrt{m}. \quad (70)$$

Assume that a n_2 -state 2NFA \mathcal{A} recognizes L^{mtwin} . According to Lemma 4, there is a DFA recognizes L^{mtwin} with $2^{(n_2-1)^2+n_2}$ states. According to Theorem 30, we have

$$2^{(n_2-1)^2+n_2} \geq 2^m \Rightarrow (n_2 - 1)^2 + n_2 \geq m \quad (71)$$

$$\Rightarrow n_2^2 > m \Rightarrow n_2 > \sqrt{m}. \quad (72)$$

Assume that a n_3 -state 2PFA \mathcal{A} recognizes L^{mtwin} with bounded error $\epsilon > 1/2$ and within polynomial expected running time. According to Lemma 5, there is a DFA solves promise problem A^{meq} with $n_3^{bn_3^2}$ states, where $b > 0$ is a constant. According to Theorem 30, we have

$$n_3^{bn_3^2} \geq 2^m \Rightarrow bn_3^2 \log n_3 \geq m \quad (73)$$

$$\Rightarrow n_3^3 > m/b \Rightarrow n_3 > \sqrt[3]{m/b}. \quad (74)$$

□

5 Concluding remarks

2QCFA were introduced by Ambainis and Watrous [3]. In this paper, we investigated state succinctness of 2QCFA. We have showed that 2QCFA can be more space-efficient than their classical counterparts DFA, 2DFA, 2NFA and polynomial expected running time 2PFA, where the superiority cannot be bounded. For any fix $m \in \mathbb{Z}^+$ and any $\epsilon > 0$, we have proved that there is an promise problem A^{meq} can be solved by 2QCFA with one-sided error ϵ with constant numbers of quantum and classical states in polynomial expected running time, whereas the sizes of the corresponding DFA, 2DFA, 2NFA and polynomial expected running time 2PFA are at least $2m + 2$, $\sqrt{\log m}$, $\sqrt{\log m}$ and $\sqrt[3]{(\log m)/b}$. We have also showed that there exists a 2QCFA \mathcal{A} recognizes language L^{mtwin} with one-sided error ϵ with constant numbers of quantum and classical states in exponential expected running time, whereas the sizes of the corresponding DFA, 2DFA, 2NFA and polynomial expected running time 2PFA are at least 2^m , \sqrt{m} , \sqrt{m} and $\sqrt[3]{m/b}$.

To conclude, we would like to propose some problems for further consideration.

1. Can promise problem A^{meq} be improved to a language?
2. In Theorem 31, we give the bound of a polynomial expected running time 2PFA. What is the bound when the expected running is exponential?

References

- [1] A. Ambainis, M. Beaudry, M. Golovkins, A. Kikusts, M. Mercer, and D. Thénrien, Algebraic Results on Quantum Automata, *Theory of Computing Systems* **39** (2006) 165–188.
- [2] A. Ambainis, R. Freivalds, One-way quantum finite automata: strengths, weaknesses and generalizations, in: *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press, Palo Alto, California, USA, 1998, pp. 332–341.
- [3] A. Ambainis, J. Watrous, Two-way finite automata with quantum and classical states, *Theoretical Computer Science* **287** (2002) 299–311.
- [4] A. Ambainis, A. Yakaryilmaz, Superiority of exact quantum automata for promise problems, *Information Processing Letters* **112** (7) (2012) 289–291. Also arXiv:1101.3837v2.
- [5] A. Ambainis, N. Nahimovs, Improved constructions of quantum automata, *Theoretical Computer Science* **410** (2009) 1916–1922.
- [6] A. Ambainis, A. Nayak, A. Ta-Shma, U. Vazirani, Dense quantum coding and quantum automata, *Journal of the ACM* **49** (4) (2002) 496–511.
- [7] A. Bertoni, C. Mereghetti, B. Palano, Quantum Computing: 1-Way Quantum Automata, in: *Proceedings of the 9th International Conference on Developments in Language Theory (DLT2003)*, Lecture Notes in Computer Science, Vol. 2710, Springer, Berlin, 2003, pp. 1–20.
- [8] J.C. Birget, State-complexity of finite-state devices, state compressibility and incompressibility. *Math. Systems Theory*, **26** (1993), pp. 237–269.
- [9] A. Brodsky, N. Pippenger, Characterizations of 1-way quantum finite automata, *SIAM Journal on Computing* **31** (2002) 1456–1478.
- [10] C. Dwork, L. Stockmeyer, A time-complexity gap for two-way probabilistic finite state automata, *SIAM J. Comput.* **19** (1990) 1011–1023.
- [11] C. Dwork, L. Stockmeyer, Finite state verifiers I: The power of interaction, *J. ACM* **39** (4) (1992) 800–828.
- [12] W. Feller, *An Introduction to Probability Theory and its Applications*, Vol. I, Wiley, New York, 1967.
- [13] J. Gruska, *Quantum Computing*, McGraw-Hill, London, 1999.

- [14] J. E. Hopcroft, J. D. Ullman, Introduction to Automata Theory, Languages, and Computation, Addison-Wesley, New York, 1979.
- [15] A. Kondacs, J. Watrous, On the power of quantum finite state automata, in: Proceedings of the 38th IEEE Annual Symposium on Foundations of Computer Science, 1997, pp. 66–75.
- [16] E. Kushilevitz and N. Nisan, Communication Complexity, Cambridge University Press, 1997.
- [17] F. Le Gall, Exponential separation of quantum and classical online space complexity, in: Proceedings of SPAA'06, 2006, pp. 67–73.
- [18] L. Z. Li and D. W. Qiu, Determination of equivalence between quantum sequential machines, Theoretical Computer Science **358** (2006) 65–74.
- [19] L. Z. Li, D. W. Qiu, Determining the equivalence for one-way quantum finite automata, Theoretical Computer Science **403** (2008) 42–51.
- [20] L. Z. Li, D. W. Qiu, X. F. Zou, L. J. Li, L. H. Wu, P. Mateus, Characterizations of one-way general quantum finite automata, Theoretical Computer Science, doi:10.1016/j.tcs.2011.10.021.
- [21] C. Moore and J. P. Crutchfield, Quantum automata and quantum grammars, Theoretical Computer Science **237** (2000) 275–306.
- [22] C. Mereghetti, B. Palano, Quantum finite automata with control language, RAIRO-Inf. Theor. Appl. **40** (2006) 315–332.
- [23] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000.
- [24] K. Paschen, Quantum finite automata using ancilla qubits, Technical Report, University of Karlsruhe, 2000.
- [25] A. Paz, Introduction to Probabilistic Automata, Academic Press, New York, 1971.
- [26] D. W. Qiu, Some Observations on Two-Way Finite Automata with Quantum and Classical States, ICIC 2008, LNCS 5226 (2008), pp. 1–8.
- [27] D. W. Qiu, L. Z. Li, An overview of quantum computation models: quantum automata, Frontiers of Computer Science in China **2** (2)(2008) 193–207.
- [28] D. W. Qiu, P. Mateus, and A. Sernadas, One-way quantum finite automata together with classical states, arXiv:0909.1428.

- [29] D. W. Qiu, S. Yu, Hierarchy and equivalence of multi-letter quantum finite automata, *Theoretical Computer Science* **410** (2009) 3006–3017.
- [30] J. Watrous, Quantum computational complexity, R.A. Meyers, Editor, *Encyclopedia of Complexity and Systems Science*, Springer (2009), pp. 7174–7201.
- [31] A. Yakaryilmaz, A. C. C. Say, Succinctness of two-way probabilistic and quantum finite automata, *Discrete Mathematics and Theoretical Computer Science* **12** (4) (2010) 19–40.
- [32] A. Yakaryilmaz, A. C. C. Say, Languages recognized by nondeterministic quantum finite automata, *Quantum Information and Computation* **10** (9-10) (2010) 747–770.
- [33] A. Yakaryilmaz, A. C. C. Say, Unbounded-error quantum computation with small space bounds, *Information and Computation* **209** (2011) 873–892.
- [34] S. Yu, Regular Languages, In: G. Rozenberg, A. Salomaa (Eds.), *Handbook of Formal Languages*, Springer-Verlag, Berlin, 1998, pp. 41–110.
- [35] S. G. Zheng, L. Z. Li, D. W. Qiu, Two-Tape Finite Automata with Quantum and Classical States, *International Journal of Theoretical Physics* **50** (2011) 1262–1281.
- [36] S. G. Zheng, D. W. Qiu, L. Z. Li, Some languages recognized by two-way finite automata with quantum and classical states, *International Journal of Foundation of Computer Science*, (to appear). Also arXiv:1112.2844.
- [37] S. G. Zheng, D. W. Qiu, L. Z. Li, Jozef Gruska, One-way finite automata with quantum and classical states, arXiv:1112.2022.